REMARKS

Claims 64-86 are pending in the present application. In the above amendments, claims 64, 72 and 77 - 82 have been amended, and claims 87-91 have been added.

Applicants respectfully respond to this Office Action.

Claim Objections

Claims 72-81 were objected for certain informalities. Claim 72 was amended to recite "securely storing". Claims 77 (and 82) were amended to recite "the mobile equipment". Claims 77-81 were amended to recite "non-transitory machine readable medium". Accordingly, the objections to claims 72-81 should be withdrawn.

Claim Rejections – 35 USC § 112

Claims 64-71 and 77-81 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite for failing to point out and distinctly claim the subject matter which applicants regard as the invention. More specifically, the Examiner asserted the claims "include limitations directed to the processing power or memory size of the respective components. However, it is unclear how or if these limitations have any effect on the scope of the method or machine readable medium claims, respectively." See, Office Action, page 4, item 6.e.

As mentioned above, claim 64 has been amended to clarify that "more" is related to "secure" rather than to "storage". Thus, the feature reciting that "key storage in the secure processing unit is more secure than key storage in the mobile equipment" allows greater security in the method of claim 64 for broadcasting encrypted multimedia content, and distinguishes the method of claim 64 from less secure methods in which key storage in the secure processing unit is not more secure than key storage in the mobile equipment. Further, Applicants can define in the claims what they regard as their invention essentially in whatever terms they choose, and all words in a claim must be considered in judging the patentability of a claim against the prior art. See, MPEP 2173.01 and 2173.06. The non-transitory machine readable medium of claim 77 is similarly distinguished.

The feature reciting that "the secure processing unit has processing power sufficient to decrypt an encrypted broadcast access key and to generate a short term key does not have processing power sufficient to decrypt encrypted multimedia content . . . wherein the terminal's secure processing unit decrypts the encrypted broadcast access key using the secure processing unit's unique private key" has a distinguishing effect over the cited U.S. Patent Application Publication No. 2002/0141591 to Hawkes et al. (the Hawkes application publication). The Hawkes application publication teaches that "[s]ymmetric encryption is generally much faster than public key encryption." See, paragraph [0047]. Thus, Applicants assert that one ordinary skill in the art would not be motivated to use asymmetric encryption in a secure processing unit that does not have sufficient processing power for certain uses. Accordingly, the processing power features of claim 64 distinguishes the claim 64 from other methods based on processing power. Further, Applicants can define in the claims what they regard as their invention essentially in whatever terms they choose, and all words in a claim must be considered in judging the patentability of a claim against the prior art. See, MPEP 2173.01 and 2173.06. The non-transitory machine readable medium of claim 77 is similarly distinguished.

Accordingly, the rejections to claims 64 and 77, and the respective dependent claims 65-71 and 78-81, under 35 U.S.C. §112, second paragraph, should be withdrawn.

Claim Rejections – 35 USC § 103

Claims 64-69, 71-75, 77-80 and 82-85 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over U.S. Patent Application Publication No. 2002/0141591 to Hawkes et al. (the Hawkes application publication) in view of U.S. Patent Application Publication No. 2006/0168446 to Ahonen et al. (the Ahonen application publication). Claims 70, 76, 81 and 86 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over the Hawkes application publication in view of the Ahonen application publication, and further in view of Applied Cryptography, Second Edition by Bruce Schneier (the Schneier publication).

The rejection of claim 64 as allegedly unpatentable over the Hawkes application publication in view of the Ahonen application publication is respectfully traversed. Claim 64, as amended, recites a method for broadcasting encrypted multimedia content over the air from a content provider to a plurality of terminals authorized based on a broadcast access key,

comprising: each terminal forwarding a unique public key over the air to the content provider, wherein each terminal has a mobile equipment and has a secure processing unit that securely stores a unique private key, corresponding to the unique public key, such that the unique private key is not accessible to the mobile equipment of the respective terminal user, key storage in the secure processing unit is more secure than key storage in the mobile equipment, the secure processing unit has processing power sufficient to decrypt an encrypted broadcast access key and to generate a short term key, the secure processing unit does not have processing power sufficient to decrypt encrypted multimedia content, and the broadcast access key is encrypted by the content provider using the unique public keys of each of the respective terminals to authorize the respective terminal to receive encrypted multimedia content, wherein the terminal's secure processing unit generates the short-term key using the broadcast access key and the short-term key information, and provides the short-term key to the terminal's mobile equipment, and each terminal's mobile equipment decrypting the multimedia content using the short-term key.

As mentioned above, claim 64 has been amended to clarify that "more" is related to "secure" (as in "more secure") rather than to "storage" (as in "more storage"). Support for the amendments to claim 64 may be located in the original specification at page 11, lines 17-24, page 12, lines 6-14, and page 13, lines 25-26.

The Examiner acknowledges that the Hawkes application publication "lacks wherein the secure processing unit stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key." See, Office Action, page 5.

Applicants assert that the Hawkes application publication fails to disclose all of the features recited in claim 64. Claim 64 specifically recites that "each terminal . . . has a secure processing unit that securely stores a unique private key, corresponding to the unique public key . . . key storage in the secure processing unit is more secure than key storage in the mobile equipment . . . ."

The Examiner asserts that the Ahonen application publication teaches a system where each terminal stores a unique private key that is similar to Hawkes's RK, a key encrypting key (KEK), decrypted using the private key, that is similar to Hawkes's BAK, and the KEK is used to decrypt a received traffic encrypting key (TEK). See, Office Action, page 6.

Applicants respectfully disagree with the Examiner's similarly assertions with respect to the keys of the Hawkes application publication and the keys of Ahonen application publication. Applicants assert that one of ordinary skill in the art would interpret the RK of the Hawkes application publication to correspond most closely to the KEK of the Ahonen application publication, and would interpret the SK of the Hawkes application publication to correspond most closely to the TEK of the Ahonen application publication. Applicants further assert that none of the keys of the Ahonen application publication has the same characteristics as the common BAK of the Hawkes application publication.

In the Hawkes application publication, the registration key (RK) is agreed upon by the CS and the UIM, and is unique to a given UIM. The registration process alone does not give the user access to a broadcast content. After registration the user subscribes to the service. In the subscription process the CS sends the UIM 308 the value of a common Broadcast Access Key (BAK). The BAK is used to derive short-term keys (SK). See, paragraph [0070]. The SK is used to decrypt the broadcast content for a short amount of time. See, paragraph [0068].

In the Ahonen application publication, the controller generates a unique KEK for the terminal, encrypts the KEK using the terminal's unique public key, and unicasts the KEK together with a new TEK (encrypted with the KEK) to the terminal. See, paragraph [0046]. The transmitted data is encrypted with a single TEK which is known to all of the receivers. See, paragraph [0007]. A public/private key pair can be used by the user to access a secure multicast/broadcast. See, paragraph [0020].

Unlike the common BAK of the Hawkes application publication, the KEK of the Ahonen application publication is unique for the terminal. Also, the RK of the Hawkes application publication encrypts the common BAK, whereas the private key of the Ahonen application publication encrypts the terminal unique KEK. Further, the RK of the Hawkes application publication does not authorize the use to access the broadcast content, whereas the public/private key pair of the Ahonen application publication can be used to access a secure multicast/broadcast. In addition, the SK of the Hawkes application publication is encrypted by the common BAK, whereas the TEK of the of the Ahonen application publication is encrypted by the terminal unique KEK. Accordingly, Applicants assert that the RK of the Hawkes application publication is not similar to the private key of the Ahonen application publication, and that the

BAK of the Hawkes application publication is not similar to the KEK of the Ahonen application publication.

In addition, the Hawkes application publication teaches that "[s]ymmetric encryption is generally much faster than public key encryption." See, paragraph [0047]. Thus, Applicants assert that one ordinary skill in the art would not be motivated to use asymmetric encryption, instead of the disclosed symmetric encryption, in a secure processing unit that does not have sufficient processing power for certain uses. Further, Applications assert that the Ahonen application publication fails to remedy this disclosure deficiency of the Hawkes application publication.

Also, the Ahonen application publication merely discloses use of the private key without disclosing secure storage of the private key in a secure processing unit wherein key storage in the secure processing unit is more secure than key storage in the mobile equipment.

For these reasons, Applicants respectfully assert that claim 64 recites patentable advances over the Hawkes application publication in view of the Ahonen application publication, and respectfully request the rejections of claim 64 be withdrawn.

It is respectfully submitted that dependent claims 65-69 and 71 are at least allowable for the reasons given above in relation to independent claim 64.

Claims 72-75, 77-80 and 82-85 are integrated circuit, machine readable medium, and apparatus claims having features defined by language similar to that of method claims 64-69 and 71. Accordingly, for the reasons recited above with respect to claims 64-69 and 71, claims 72-75, 77-80 and 82-85 define patentable advances over the Hawkes application publication in view of the Ahonen application publication, and the rejections of claims 72-75, 77-80 and 82-85 should be withdrawn.

The rejections of claims 70, 76, 81 and 86 as being unpatentable over the Hawkes application publication in view of the Ahonen application publication, and further in view of the Schneier publication, are respectfully traversed. Claims 70, 76, 81 and 86 incorporate all of the features of independent claims 64, 72, 77 and 82, respectively. Applicants assert that the Schneier publication fails to remedy the disclosure deficiencies of the Hawkes and Ahonen patent publications as described above with respect to claim 64. Accordingly, Applicants respectfully request the Examiner to withdraw the rejections of claims 70, 76, 81 and 86.

New Claims

New claims 87-91 are method claims having features similar to the features of method claims 64-65 and 68-71, with a perspective more aligned with a terminal. Accordingly, it is respectfully submitted that claims 87-91 are at least allowable for the reasons given above in relation to claims 64-65 and 68-71.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **July 30, 2010**

By: Won Tae C. Kim
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502